



U.S. Department of Justice

Executive Office for Immigration Review

Office of the General Counsel

5107 Leesburg Pike, Suite 2150
Falls Church, Virginia 22041

June 17, 2019

Matthew Hoppock
MuckRock News
DEPT MR 69766
411A Highland Ave
Somerville, MA 02144-2516

Re: FOIA 2019-21471

Dear Mr. Hoppock,

This letter is in response to your Freedom of Information Act (FOIA) request to the Executive Office for Immigration Review (EOIR) in which you seek documents posted to the BIA intranet.

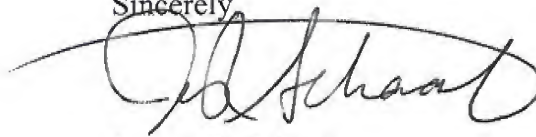
Responsive documents are enclosed. Portions of the enclosed documents have been redacted in accordance with 5 U. S.C. § 552(b)(6) to avoid a clearly unwarranted invasion of personal privacy, 5 U. S.C. § 552(b)(5) to protect privileged information, and/or 5 U. S.C. § 552(b)(7) to protect law enforcement information. The reason for redaction is clearly marked on each redacted portion.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. *See* 5 U.S.C. § 552(c) (2006 & Supp. IV 2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. *See* <http://www.justice.gov/oip/foiapost/2012foiapost9.html>.

You may contact our FOIA Public Liaison at the telephone number 703-605-1297 for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, Room 2510, 8601 Adelphi Road, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

If you are not satisfied with my response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, DC 20530-0001, or you may submit an appeal through OIP's FOIAonline portal by creating an account on the following web site: <https://www.foiaonline.gov/foiaonline/action/public/home>. Your appeal must be postmarked or electronically transmitted within 90 days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

Sincerely,

A handwritten signature in black ink, appearing to read "J. Schaaf", with a large, sweeping flourish extending from the end of the signature.

Joseph R. Schaaf

Senior Counsel for Administrative Law



BOARD OF IMMIGRATION APPEALS (BIA) INFORMATION TECHNOLOGY OFFICE (ITO)

The ITO is available to assist with computer related issues.

Questions eMail the [BIA ITO Staff \(EOIR\)](#).

Issues, eMail the [Service Desk](#), and CC the BIA TIO Staff (EOIR).

Please note: The BIA ITO is NOT part of the Service Desk and the Service Desk does not work for ITO. The ITO is the Boards' liaison to the Office of Information Technology (OIT) and the Service Desk.

Throughout the year, the ITO holds **Technology Sessions**. These sessions are meant to keep BIA staff informed about:

- Upcoming computer projects affecting Board Staff
- Recent computer issues, and their status
- Upcoming changes to BIA computer systems
- Address BIA staff questions
- Provide Helpful Hints

The Administrative staff and the **ITO** are responsible for submitting computer related requests. Requests include, but are not limited to:

- CASE Account
 - Please note, Jeff Sykes submits the initial NT Account requests.
- FileTrail
- eTranscription
- Electronic En Banc
- Cognos
- Software installation

Should you have issues with any of the above, please eMail the [BIA ITO Staff \(EOIR\)](#).

If you are not sure if a request should be addressed to the BIA ITO or Jeff Sykes, please e-mail [both](#), and we will determine who the proper party is to address the request.

The ITO also creates **Quick Reference Guides (QRGs)** and **Helpful Hints (HHs)** for BIA Staff to refer to. If there are frequent issues that BIA Staff encounter, the BIA ITO will generate a guide for all to use.

COMPUTER & TECHNOLOGY SOLUTIONS

| For help with ... | Contact ... |
|--------------------------------------|--|
| CASE | eMail BIA ITO Staff, BIAITOSTaffEOIR@coar.usdoj.gov . |
| Drives | See "User account issues". |
| Equipment (computer, phone, etc.) | <p>For Clerk's Office staff, contact Sheridan Butler, (b) (6)</p> <p>(b) (6)</p> <p>For legal and other BIA staff, contact Jeff Sykes, (b) (6)</p> <p>(b) (6)</p> |
| General computer issues | <p>Call the EOIR Service Desk at (703) 305-7347, or</p> <p>Email OITServiceDesk@usdoj.gov, with a cc: to (1) BIA ITO Staff, (2) Donna Carr, and (3) Jeff Sykes.</p> |
| Outlook | See "User account issues". |
| Software request | eMail BIA ITO Staff, BIAITOSTaffEOIR@coar.usdoj.gov . |
| User account issues | <p>For Clerk's Office staff, contact Sheridan Butler, (b) (6)</p> <p>(b) (6)</p> <p>For legal and other BIA staff, contact Jeff Sykes, (b) (6)</p> <p>(b) (6)</p> |
| When in doubt / everything else | <p>If it's a physical item (like you need a new computer part or telephone), contact Jeff Sykes, (b) (6) (b) (6)</p> <p>If it's a technical problem (like a program not working or help with a report), email BIA ITO Staff, BIAITOSTaffEOIR@coar.usdoj.gov.</p> |

**Executive Office for Immigration Review (EOIR)
Cybersecurity and Privacy
Rules of Behavior (ROB) for Information Technology Systems**

I. Introduction

These Rules of Behavior (ROB) for General Users pertain to the use, security, and acceptable level of risk for EOIR systems and applications. Each EOIR user is responsible for the security and privacy of DOJ information systems and their data. As a user of the EOIR information systems and data, each user serves as the first line of defense in support of EOIR's cybersecurity protections and enforcement of appropriate privacy protections for Personally Identifiable Information (PII).

The intent of the ROB is to acknowledge receipt and understanding by EOIR users of applicable cybersecurity requirements and responsibilities (as detailed in Federal and DOJ policies and procedures). These requirements include, but are not limited to, the Office of Management and Budget (OMB) Circular A-130, OMB M-17-12, OMB M-16-24, the Privacy Act of 1974, DOJ Order 0904 Cybersecurity Program, DOJ Order 0601 Privacy and Civil Liberties, DOJ Order 2740.1 (series), and the DOJ Cybersecurity Standard.

Who is covered by these rules?

The ROB is to be followed by all EOIR users (i.e., government employees, interns, contractors, student workers, volunteers, and personnel supplying services) who use any computing resources that support the mission and functions of the Department of Justice and EOIR. All individuals must be trained on the ROB prior to being granted access to the information technology system. New employees must sign the ROB with a wet signature during their initial onboarding. Thereafter, all users are required to review and confirm that they have read, understand and acknowledge these rules during the annual Cybersecurity Awareness Training conducted through LearnDOJ.

When authorized, users may obtain limited exemptions from particular terms of these ROB for specific occurrences when necessary for performance of official duties. These individual exemption requests must document why a particular rule prevents or hinders mission operations. The information system Authorizing Official (AO) has the ability to issue an exemption if the accepted risk(s) and justification are appropriate, substantiated and documented.¹

In addition to this ROB, users with escalated privileges on an information system (e.g., administrator) must also agree to and provide signature or electronic verification acknowledging compliance for the Privileged User ROB.

¹ For additional information on mobile device exemptions, please refer to the *Department of Justice Mobile Device and Mobile Application Security Policy Instruction v5* (https://dojnet.doj.gov/jmd/ocio/ocio-document_library/es/2-DOJ_Policy_Instruction/Mobile_Device_and_Mobile_Application_Security_Policy_Instruction_v5.pdf).

**Executive Office for Immigration Review (EOIR)
Cybersecurity and Privacy
Rules of Behavior (ROB) for Information Technology Systems**

Users will be held responsible for compromising Government information through negligence or willful act. Users must use caution and follow all statutory and regulatory access restrictions, as well as adhere to Department and Component level policies on limitations on the exchange of access-restricted information such as taxpayer, personally identifiable, controlled unclassified, and grand jury information. Failure to comply with the rules and responsibilities listed in this ROB may result in appropriate sanctions, including but not limited to: remedial training; loss of access to information; loss of a security clearance; verbal or written warning; termination of employment; or civil or criminal prosecution.

II. User Responsibilities

A. General

1. Comply with all Federal laws and Department and Component policies and requirements, including DOJ Orders, Policy Statements, and Standards. Use DOJ information and information systems for lawful, official use, and authorized purposes only.
2. Ensure individuals have the proper clearance, authorization, and need-to-know before providing access to any DOJ information.
3. Read and accept the DOJ security warning banner that appears prior to logging onto the system or mobile device. Acknowledgment of this ROB also indicates consent to monitoring, recording, and collection of data on all DOJ devices for law enforcement purposes.
4. Consent to the monitoring and search of any IT equipment brought into, networked to, or removed from DOJ owned, controlled, or leased facilities consistent with employee and contractor consent obtained through logon banners and DOJ policies.
5. Screen-lock or log off, and remove the personal identity verification (PIV) card from your computer when leaving the work area.
6. Keep your PIV card on you when not in use for authentication, and keep it out of sight when away from the worksite area.
7. Do not generate, view, download, store, copy, or transmit offensive or inappropriate information in any medium, to include email messages, documents, images, videos, and sound files (e.g., graphic violence, pornography, hateful language, etc.).
8. Do not access continuous data streams such as viewing streaming video or listening to streaming audio/radio on a website on Department computers and computer systems during working or nonworking hours.

Executive Office for Immigration Review (EOIR)
Cybersecurity and Privacy
Rules of Behavior (ROB) for Information Technology Systems

9. Adhere to Separation of Duties principles. Avoid conflict of interest in responsibilities, roles, and functions within a system or application (e.g., duties of the System Administrator and Database Administrator should not be combined).
10. Do not use anonymizer sites on the internet and bypass the Department security mechanisms designed to protect systems from malicious internet sites.
11. Do not use Peer-to-Peer (P2P) technology (e.g., BitTorrent) on the internet unless the Department's Chief Information Officer (CIO) or designee approves a waiver from the Department policy.
12. Do not post Department information on cloud-based services unless approved by the Component CIO or designee.
13. Do not post Department official business information on public websites or social media unless in accordance with applicable Departmental and Component level policies and explicitly authorized for your official duties (e.g., Public Affairs Office).
14. Do not post information on social media or public websites which allows unauthorized users to infer or obtain non-public information (e.g., system account information, sensitive personally identifiable information (PII), project status, etc.).
15. Upload only the user's picture as a profile picture in Outlook. User's picture must be in a professional pose from the shoulders up with the U.S. flag or a neutral background.
16. Protect and safeguard all DOJ information commensurate with the sensitivity and value of the data at risk, including encrypting all sensitive PII before sending to third parties outside of DOJ.
17. Protect and safeguard all DOJ information and information systems from unauthorized access; unauthorized or inadvertent modification, disclosure, damage, destruction, loss, theft, denial of service; and improper sanitization or use.
18. Ensure that all DOJ data on authorized removable media (e.g., thumb drives, removable hard drives, and CD/DVD), laptops, tablets, and mobile devices (e.g., smartphones and netbooks) is encrypted with a Department-approved solution unless the Department's CIO or designee approves a waiver from the Department policy.
19. Handle all Department data as Sensitive unless designated as Non-Sensitive by the Component Head or Office Director.
20. Report any anomalous unusual behavior, breaches in security, data spills and discovered or suspected security incidents within one (1) hour of discovery to the OIT Service Desk

**Executive Office for Immigration Review (EOIR)
Cybersecurity and Privacy
Rules of Behavior (ROB) for Information Technology Systems**

(OITServiceDesk@EOIR.USDOJ.GOV) for the System Security & Integrity Staff (SSIS) to report to DOJCert@usdoj.gov.

21. Ensure that you complete any required training in accordance with current Department policies.
22. Follow all Department level and Component level policies related to user responsibilities for the recording of information into the Department's recordkeeping systems, and comply with applicable records retention schedules.

B. Classified Systems/Information

23. Do not use portable electronic devices (e.g., smart watches, fitness trackers, laptops, mobile devices, and removable media except CD-R for music) in sensitive compartmented information facilities or areas where classified information processing is authorized.²
24. Properly mark and label classified and sensitive documents, electronic equipment, and media.³
25. Do not process classified information on an unclassified system.
26. For classified environments, follow the procedures required for those networks for data storage and transport. Do not send classified emails on an unclassified system or use authorized devices without the appropriate level of security classification.
27. Operate information systems only in areas certified for the highest classification or sensitivity level of the information being processed. When not in use, classified items should be stored and contained in an approved security facility.⁴
28. Receive the proper security training before handling classified removable media. Transport classified removable media only when authorized.

² For additional information on authorized use of PEDs when working in spaces authorized to process classified information, please refer to *DOJ Order 0904* (<https://portal.doj.gov/sites/dm/dm/Directives/0904.pdf>), *DOJ Security Program Operating Manual (SPOM) Chapter 8* (<http://dojnet.doj.gov/jmd/seps/spom/chapter8.pdf>), and *Intelligence Community Directive 503* (http://www.dni.gov/files/documents/ICD/ICD_503.pdf).

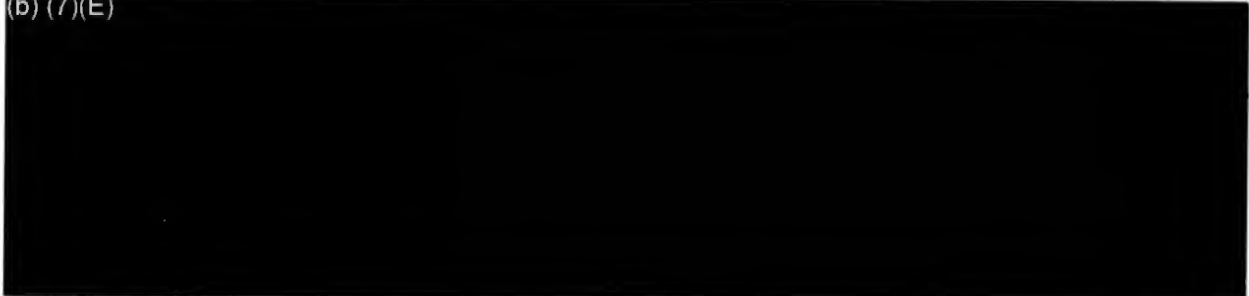
³ For additional instruction on proper markings, please refer to the *DOJ Security Program Operating Manual (SPOM)* (<https://dojnet.doj.gov/jmd/seps/spom.php>).

⁴ For additional information on removable media, please refer to the *DOJ Removable Media Requirements for Classified Systems* (https://dojnet.doj.gov/jmd/seps/docs/removable_media_requirements.pdf).

Executive Office for Immigration Review (EOIR)
Cybersecurity and Privacy
Rules of Behavior (ROB) for Information Technology Systems

C. Passwords

(b) (7)(E)



D. AVAILABILITY

- 33. Plan for contingencies such as disaster recovery, loss of information, and disclosure of information by preparing alternate work strategies and recovery mechanisms. Be familiar with the part you play in local contingency plans.
- 34. Save files to your assigned home directory which is your H:\ drive or shared network drives. This is backed up daily on the network.
- 35. Do not store files to the C:\ drive. These files are not backed up daily to the network.
- 36. Store backups away from originals.
- 37. Protect storage media from spills of food and drink.

E. Hardware

- 38. Do not add, modify, or remove hardware, or connect unauthorized accessories or communications connections to DOJ resources unless specifically authorized.
- 39. Do not access the internal components of the computer or its hard drive from DOJ facilities, unless specifically authorized.
- 40. There is no expectation of maintaining any personal information, data, or applications on DOJ systems, networks or devices.

F. Software

- 41. Do not copy or distribute intellectual property without permission or license from the copyright owner (e.g., music, software, documentation, and other copyrighted materials). Use only DOJ-licensed and authorized software.

**Executive Office for Immigration Review (EOIR)
Cybersecurity and Privacy
Rules of Behavior (ROB) for Information Technology Systems**

- 42. Do not install or update any software unless specifically authorized. Submit requests for system changes through the OIT Service Desk (OITServiceDesk@EOIR.USDOJ.GOV) or configuration management process.
- 43. Do not attempt to access any electronic audit trails that may exist on the computer unless specifically authorized.
- 44. Do not change any configurations or settings of the operating system and security-related software, or circumvent and test the security controls of the system unless authorized through the documented configuration management procedures.

G. Email Use

- 40. Limit distribution of email only to those with a need-to-know.
- 41. Do not open emails from suspicious sources (e.g., people you do not recognize, know, or normally communicate with) or click on links embedded in these emails, simply forward to phishing@usdoj.gov and do not visit untrusted or inappropriate websites (unless authorized).
- 42. Do not open emails that contain unsolicited advertisements, simply forward these emails to Ex_DOJMAILSPAM@jmd.usdoj.gov. Download permissible files only from known and reliable sources and use virus- checking procedures prior to file use.
- 43. Do not auto-forward emails from your DOJ email account to or through a non-DOJ email system (e.g., Gmail, Yahoo, and Outlook.com).
- 44. Comply with [DOJ Policy Statement 0801.04](#), Electronic Mail and Electronic Messaging Policy Statement, on the appropriate capture of email.
- 45. Do not use personal email accounts for DOJ business except under exigent circumstances and in accordance with Policy Statement 0801.04, Electronic Mail and Electronic Messaging Policy Statement, and any Component-level policy related to the use of personal email accounts.

H. Mobile Computing and Remote Access⁵

- 45. Use mobile Government Furnished Equipment (GFE) (e.g., laptop, tablet, smartphone) for official business and authorized use in accordance with the *de minimis* rule. Mobile GFE is

⁵ For additional information, please refer to the [DOJ Mobile Device and Mobile Application Security Policy Instruction](https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/Mobile_Device_and_Mobile_Application_Security_Policy_Instruction_v5.pdf) (https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/Mobile_Device_and_Mobile_Application_Security_Policy_Instruction_v5.pdf).

Executive Office for Immigration Review (EOIR)
Cybersecurity and Privacy
Rules of Behavior (ROB) for Information Technology Systems

for use by DOJ personnel only and shall connect to DOJ networks only through an approved DOJ remote access method.

46. Keep all GFE mobile devices, portable electronic devices and removable media assigned to you in your physical presence whenever possible, and/or secured out of sight.
47. Do not bypass native mobile device operating system controls to gain increased privileges (e.g., jailbreaking or rooting the device).
48. Download and/or install only authorized applications and software on DOJ mobile devices, and only from DOJ-authorized sources.
49. Install DOJ-provided removable media, including memory (such as SD cards) and subscriber identity module cards, only on GFE mobile devices.
50. Immediately report lost or stolen devices (e.g., laptop, phone, tablet, thumb drive) to the EOIR OIT Service Desk (OITServiceDesk@EOIR.USDOJ.GOV) for SSIS to report the incident to JSOC.
51. Do not associate a personal gift or credit card with a government app store account (e.g., iTunes or Google Play). Authorized mobile application purchases should be made by the appropriate contracting officer or official designee (e.g., government purchase card holder).
52. **Unless explicitly authorized by the AO for mobile devices**, follow these rules:
 - a. Do not connect non-DOJ mobile devices and/or accessories to DOJ networks, with the exception of Guest Networks.
 - b. Do not use non-Government-approved cloud-based services (e.g., DropBox and iCloud) on mobile GFE or to transfer DOJ data.
 - c. Do not connect mobile GFE to non-DOJ information systems, to include personal computers.
53. Follow your organization's telework guidelines when working remotely and/or remotely accessing DOJ information remotely.
54. Ensure the confidentiality of government information when using remote access from a non-GFE device (public or private). As per the DOJ Strong Authentication Plan (https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/doj-strong-authentication-plan.pdf), this includes the following:
 - a. Non-GFE devices and computers must have updated antivirus, local firewall, updated OS and software patch levels.

**Executive Office for Immigration Review (EOIR)
Cybersecurity and Privacy
Rules of Behavior (ROB) for Information Technology Systems**

- b. In addition, all wireless access to DOJ networks must be from a Wi-Fi Protected Access 2 (WPA2) or higher encrypted wireless network.

I. Virtual Conferencing

- 55. Hosts and presenters must provide participants with advance notice if the virtual conference session is being recorded.
- 56. Do not access a virtual conference presentation using a privileged user account.
- 57. Limit presentation information to only that which is authorized for dissemination.
- 58. Delete all DOJ information on a provider's web site immediately upon the end of a virtual conference.
- 59. Do not install any agents or other software designed to enhance or aid in virtual conferencing. Submit requests for system and software changes through the appropriate OIT Service Desk (OITServiceDesk@EOIR.USDOJ.GOV) or configuration management process.
- 60. Employ strong participant authentication mechanisms (e.g., multi-factor authentication, PIN creation, unique login credentials).
- 61. Users are provided with logging, auditing, and the appropriate/authorized meeting functions (e.g., upload, download, desktop sharing).

J. Traveling Users

- 62. Adhere to the Department requirements and recommendations regarding foreign travel and mobile devices in the *DOJ Mobile Device and Mobile Application Security Policy Instruction*.⁶
- 63. Prior to traveling abroad to a foreign country, notify the OIT Service Desk (OITServiceDesk@EOIR.USDOJ.GOV) that you plan to bring mobile GFE devices such as your laptop, smartphone and/or tablet and provide dates and location(s) to include city and country of travel for authorization and approval.. SSIS will then notify JSOC (DOJCert@usdoj.gov) of your travel plans. The DOJ Chief Information Security Officer must

⁶ For additional information on traveling with a mobile device, please refer to *the DOJ Mobile Device and Mobile Application Security Policy* Instructions (https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/Mobile_Device_and_Mobile_Application_Security_Policy_Instruction_v5.pdf).

**Executive Office for Immigration Review (EOIR)
Cybersecurity and Privacy
Rules of Behavior (ROB) for Information Technology Systems**

approve the use of laptops for any foreign travel and mobile devices to countries designated as high-risk.⁷

64. The OIT Service Desk (OITServiceDesk@EOIR.USDOJ.GOV) must inspect computers, smartphones, and any other media that have been transported outside the United States for compromise prior to any physical or logical connection to any DOJ system.
65. Minimize the information on your information system to what is required to perform a particular mission while traveling and destroy copies of sensitive data when no longer needed.
66. Shut down devices when not in use or no longer needed. If the device is needed but not the associated network capability, turn off/disable the network/wireless network functionality.
67. Assume all communications (including cellular services) are intercepted and read when on travel in a foreign country.
68. Keep your remote access token separate from the laptop/tablet (preferably on you) when possible.

K. Personally Identifiable Information (PII)

69. Verify each computer-readable data extract containing sensitive PII data has been erased within 90 days of origination or that its use is still required.
70. Safeguard against breaches of information involving PII, which refers to information which can be used alone or combined with other information that can distinguish or trace an individual's identity—such as a name, Social Security number, Alien Registration Number (A number), biometric record, the date and place of birth, mother's maiden name, etc.
71. Report all suspected or confirmed breaches of information involving PII, consistent with DOJ, NIST, and US-CERT notification guidelines and procedures, to OIT Service Desk (OITServiceDesk@EOIR.USDOJ.GOV) to escalate the breach to SSIS for reporting to JSOC through your Component's standard incident response procedures, within one (1) hour or as possible without unreasonable delay, and consistent with DOJ, NIST, and US-CERT notification guidelines and procedures⁸.

⁷ For additional information on foreign travel requirements, please refer to the *DOJ IT Resources Outside U.S. Territory Waiver Request* form (https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/foreign_travel_it_resources_1_2.pdf).

⁸ To report a suspected or confirmed breach of information involving PII to JSOC, please email DOJCERT@usdoj.gov or report through any other means approved by the Department.

Executive Office for Immigration Review (EOIR)
Cybersecurity and Privacy
Rules of Behavior (ROB) for Information Technology Systems

- 72. Access, maintain, store, or transmit PII to which you are given explicit authorization, and ensure you meet required security controls.⁹
- 73. Disclose PII in accordance with appropriate legal authorities and the Privacy Act of 1974.
- 74. Dispose of and retain records in accordance with applicable record schedules, National Archives and Records Administration guidelines, and Department policies.¹⁰
- 75. Do not perform unauthorized querying, review, inspection, or disclosure of Federal Taxpayer Information.¹¹

⁹ For additional guidance on PII, please refer to *Cybersecurity Program, DOJ Order 0904* (<https://portal.doj.gov/sites/dm/dm/Directives/0904.pdf>) and *Privacy and Civil Liberties, DOJ Order 0601* (<https://portal.doj.gov/sites/dm/dm/Directives/0601.pdf>).

¹⁰ For disposal guidance, please refer to *Record Management, DOJ Order 0801* (<https://portal.doj.gov/sites/dm/dm/Directives/0801.pdf>).

¹¹ For additional information on disclosure of federal taxpayer information, please refer to *Internal Revenue Code Sec. 7213 and 7213A* (http://www.irs.gov/irm/part11/irm_11-003-001.html#d0e176).

**Executive Office for Immigration Review (EOIR)
Cybersecurity and Privacy
Rules of Behavior (ROB) for Information Technology Systems**

III. Statement of Acknowledgement

I acknowledge receipt and understand my responsibilities as identified above. Additionally, I acknowledge my responsibility to protect all PII I handle. I will comply with the EOIR Cybersecurity ROB for General Users, Version 2.5, dated February 06, 2019. I acknowledge that failure to comply with the ROB may result in appropriate sanctions, including but not limited to: remedial training; verbal or written warning; loss of access to information systems; loss of a security clearance; termination of employment; or civil or criminal prosecution.

Signature

Date

Printed Name

Component and Sub-Component

Note: Statements of acknowledgement may be made by signature if the ROB for General Users is reviewed in hard copy or by electronic acknowledgement if reviewed online. All users are required to review and provide their signature or electronic verification acknowledging compliance with these rules. Users with privileged accesses and permissions shall also agree to and sign the ROB for Privileged Users. If you have questions related to this ROB, please contact OIT Service Desk (OITServiceDesk@EOIR.USDOJ.GOV), Security Manager, or Supervisor.

The Department has the right, reserved or otherwise, to update the ROB to ensure it remains compliant with all applicable laws, regulations, and DOJ Standards. Updates to the ROB will be communicated through the Department's Training Team Lead and Component Training Coordinators.



HELPFUL HINTS FOR THE EOIR BARCODE SYSTEM

The following describes how to Scan Files.

HOW DO I...SCAN FILES?

There are numerous ways to scan. Support staff scan a high volume of files and have a ScanSheet to quickly scan these files. If you do not have a ScanSheet, or if you are scanning to someone not on your ScanSheet, follow these steps:

1. **View My Cart** is where scanning activities begin. To start View My Cart:
 - Log into CASE and access the **Other Programs** module.
 - From Other Programs, find the row for **Barcode Search** and click on Click to Launch.
 - Once Barcode Search loads, click the **View My Cart** button.
2. Within **View My Cart** is where you scan the files. To do this:
 - **HINT:** Verify the cursor is in the box labeled **Scan Barcode** or **RFID**. If not, click in the box to get the cursor there then begin scanning.
 - **Scan the barcodes.** Like the old system, scan all barcodes in the file.
 - Verify all barcodes appear in the cart scan window then click the **Check Out** button.
3. The **Check Out** screen is where you pick the destination. To do this:
 - From the Check Out window, select the **Location** first (even though it is second in order on the screen). The Location is like the old "Functional Level" with the Atty Team or Designated Area. All attorneys are under their Atty Team now.
 - Select the **Check Out To** field (the first field). The Check Out To field is like the old "Responsible Party" field. Attorney Home and Office are examples of Check Out To fields. The Check Out To field is filtered by the Location (e.g. Attorneys show up on their Team).
 - Verify all barcodes are there then click on the **Check Out** button to complete the move. The screen closes and the files have been moved.

HINT: On the Check Out screen, if you uncheck the **Remove from Cart when finished** box before you click the **Check Out** button, you see the details of the move. *If you do this, you must manually click the **Remove** button before scanning another set of files, so that you don't move the files again.*

HINT: On the Check Out screen, the red '**R**' means required. Do not use the "Due Back Date" field.

HINT: Do not use "Check In" because at EOIR we are only using the "Check Out" functionality.



HELPFUL HINTS FOR THE EOIR BARCODE SYSTEM

The following describes how to View Location History and See the Location in Case Manager.

HOW DO I... VIEW LOCATION HISTORY AND SEE THE LOCATION IN CASE MANAGER?

There are several ways to see the location in CASE. To see the location, follow one of these steps:

1. **View Location History.** To see the location this way:
 - Log into CASE and access the **Other Programs** module.
 - From Other Programs, find the row for **Barcode Search** and click on [Click to Launch](#).
 - Scan the ROP 1 barcode, or enter the A-Number, and click **Search**.
 - The results are shown with the most recent location. Check the box beside the A-Number and click on the **View History** icon (the Green H) at the top of the screen to see the history since it has been moved around via the new EOIR Barcode System.
2. **See the Location in Case Manager.** To see the location this way:
 - Log into CASE and access the **Case Manager** module.
 - From Case Manager, search for the A-Number.
 - Click on the appropriate hyperlink to open it (e.g. the Case Appeal link).
 - Once opened, the Location is displayed in the grey areas at the top of the screen.

HINT: In the upper grey area, the ROP Location = The location of the file at the Court. In the lower grey area, the BIA ROP Location = The location of the specific Board matter you opened (e.g. Case Appeal). When that matter is pending before the Board, the ROP Location and the BIA ROP Location will match. Once a matter is completed at the Board (e.g. a Decision is entered for a Case Appeal) use the Barcode Search (#1, above) to see the most recent location.



EXECUTIVE OFFICE FOR IMMIGRATION REVIEW
New EOIR Barcode System – Transition Aid

Streamlining Assignment Guide for the EOIR Barcode System

STREAMLINING ASSIGNMENT GUIDE FOR THE EOIR BARCODE SYSTEM

The following describes how to utilize Streamlining Assignment.

HOW DO I...ASSIGN CASES?

Various Board personnel perform Streamlining Assignment. To assign cases, follow these steps:

1. Log into **CASE** and access the **Other Programs** module.
 - From Other Programs, select **Streamlining Assignment** and click on Click to Launch.
2. Within **Streamlining Assignment**, select the Attorney from the **Please select an Attorney** list.
 - Click **Continue**.
 - Verify the cursor is in the **Scan Barcode or RFID** box. If not, click in the box.
 - **Scan all barcodes** in the file(s).
 - Verify all barcodes appear in the cart scan window. Click the **Check Out** button.
3. From the **Check Out** window, select the **Location** field. Make your selection.
 - Select the **Check Out To** field. Make your selection.
 - Uncheck the **Remove from Cart when finished** box.
 - Click the **Check Out** button.
4. Click the **ASSIGN/REFRESH** button. The case(s) will appear in the fields **Assigned** or **Rejected**.
 - If cases appear in the **Assigned** field, the assignment is complete.
 - If cases appear in the **Rejected** field, address the reasons specified.
 - If cases appear in neither field, click the **Check Out** button.
 - From the **Check Out** window, select the **Location** field. Select **A Streamlining Error**.
 - Select the **Check Out To** field. Select **BIA A Streamlining Error/A Streamlining Error**.
 - Uncheck the **Remove from Cart when finished** box.
 - Click the **Check Out** button.
 - Verify all barcodes appear in the cart scan window. Click the **Check Out** button.
 - Repeat the entire process indicated in **Step 3**.
 - Click the **ASSIGN/REFRESH** button. The assignment is complete.

Reminder: You must click the **Remove** button before assigning another set of files, so that you don't assign the files again.



Executive Office for Immigration Review Guide to Using FileTrail

How to Track ROPs

HOW TO TRACK ROPs IN FILETRAIL

Tracking ROPs in FileTrail is an essential research tool for any component at EOIR. Using the View History icon within FileTrail to track ROPs gives employees a quick way to view current and past locations dating from March 4, 2013.

STEP 1

Log into CASE

STEP 2

Click on Other Programs

STEP 3

Click on Barcode Search (Click to Launch)



Executive Office for Immigration Review Guide to Using FileTrail

How to Track ROPs

STEP 4

Enter the
A-Number in
the dialog box.



Then, click
Search

STEP 5

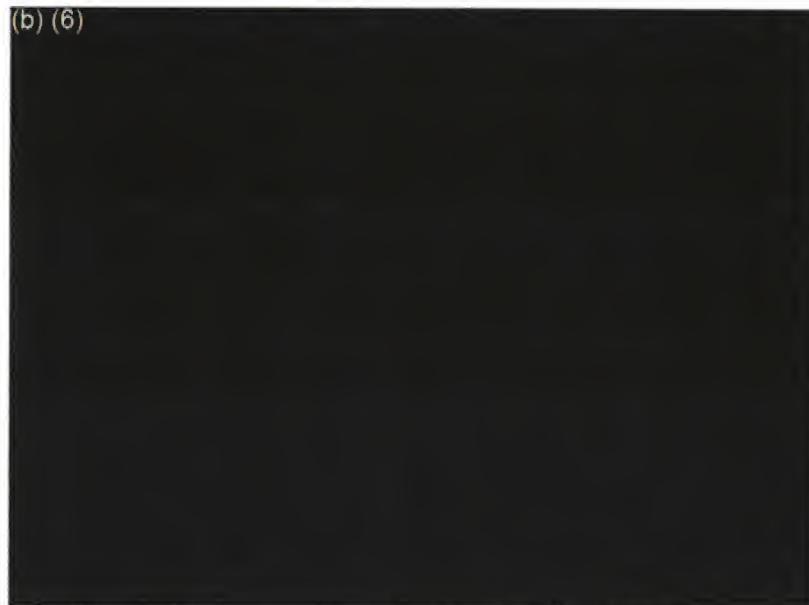
Click the box
next to the
A-Number
(use **ROP 1**)
you want to
track.



Then, click
View History
(under the
Physical
Items tab).

STEP 6

The View
History
results will
display.





Executive Office for Immigration Review
Board of Immigration Appeals

How To use Snag-It – April 8, 2016

THIS DOCUMENT WILL TEACH YOU HOW CAPTURE A SCREEN SHOT USING THE SNAGIT APPLICATION.

STEP 1

The screen capture button for Snag-it may appear at the top of your desktop screen.

When you hover over the button, more options will appear.



If the button does NOT appear at the top of your screen, open Snag-It from the Start Menu.

Click **Start**.

Select **All Programs**.

Select the **TechSmith** folder.
Click on **Snagit**.

The **Snag-it** button will appear at the top of your desktop screen.



STEP 2

Click the **Screen Capture** button.



STEP 3

Yellow cross-hairs will appear.

Place the cursor at one corner of the image.

Click and hold the left mouse button.

Drag the cursor to the opposite corner of the image.

Once you have selected the desired area, release the left mouse button.





**Executive Office for Immigration Review
Board of Immigration Appeals**

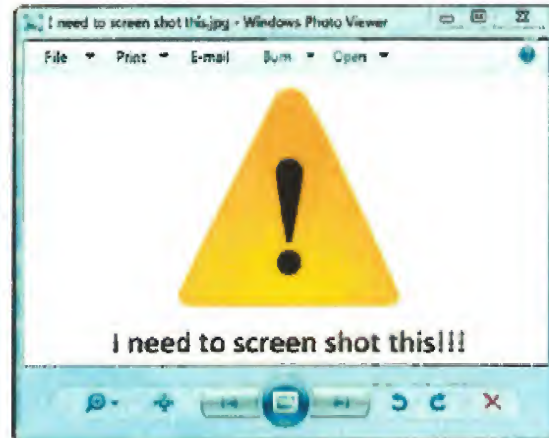
How To use Snag-It -- April 8, 2016

STEP 4

The image will appear in the **Snagit Editor** window.

From this window:
Right-Click on the image and select **Copy**.

Open the desired location (i.e. Word, eMail, etc.), and **Paste** the image.





**Executive Office for Immigration Review
Board of Immigration Appeals**

Frequently Asked Questions (FAQs) Office 2016 – April 2017

The following are Frequently Asked Questions (FAQs) related to Office 2016. If there are any questions and/or comments regarding using Microsoft Office 2016 please contact the [BIA ITO Staff](#).

Contents

| | |
|--|----------|
| Microsoft Office 2016 Overall..... | 2 |
| What happened to the Yellow Outlook Icon? | 2 |
| How do I “Pin” items to the Taskbar or Start Menu? | 2 |
| How do I add a Shortcut to my desktop? | 2 |
| What happened to the File tab?..... | 2 |
| How do I change the Spelling and Grammar settings? | 2 |
| How do I change the background color? | 3 |
| Outlook..... | 3 |
| How do I get my “Search” feature to work? | 3 |
| How do I set Outlook to “Pop-Out” an eMail reply by default? | 3 |
| How do I see messages Older than 12 months?..... | 4 |
| Microsoft Word | 4 |
| Why is my document in Protected View and how do I turn it off? | 4 |
| How do I edit Read Only Documents? | 4 |
| How do I view Track Changes? | 4 |
| How do I save a document or folder as a Favorite?..... | 5 |
| Lync is now Skype..... | 5 |



Microsoft Office 2016 Overall

What happened to the Yellow Outlook Icon?

The **Outlook** icon is now **Blue** instead of Yellow.

You can find this icon on your desktop on in the Start  Menu.



How do I "Pin" items to the Taskbar or Start Menu?

Any application you frequently use can be "pinned" to your Taskbar or Start Menu.

1. Navigate to the item you'd like to "Pin" to the Taskbar or Start Menu.
2. Right-Click on the item.
3. Select the desired location you'd like to "pin" the item to.

Open

Troubleshoot compatibility

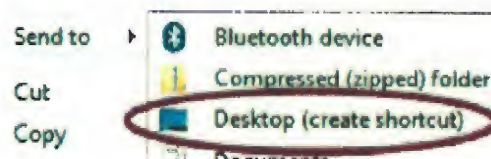
Pin to Taskbar

Pin to Start Menu

How do I add a Shortcut to my desktop?

You can create a shortcut for a file or application for easy access from your desktop. To create a shortcut:

1. Navigate to the item you'd like to create a shortcut for.
2. Right-Click on the item.
3. Select "Send to", then select **Desktop (create shortcut)**.



What happened to the File tab?

After clicking on the **File** tab, instead of showing **File** at the top, there is a **Back Arrow** which will allow you to navigate back to the previous Ribbon Tabs.



How do I change the Spelling and Grammar settings?

Check your Spelling & Grammar check settings.

1. Under the **File** tab, select **Options**.
2. Select **Proofing**.
3. Under "When correcting spelling in Microsoft Office programs" select the desired settings.
4. Under the "When correcting spelling and grammar in Word" section, the recommended setting is **Grammar Only**.

When correcting spelling in Microsoft Office programs

- Ignore words in ALL CAPS
- ✓ Ignore words that contain numbers
- ✓ Ignore Internet and file addresses
- ✓ Flag repeated words
- Enforce accented uppercase in French
- Suggest from main dictionary only

When correcting spelling in Outlook

- ✓ Check spelling as you type
- ✓ Mark grammar errors as you type
- ✓ Frequently confused words
- ✓ Check grammar with spelling
- Show readability statistics

Writing Style: **Grammar Only**

Settings

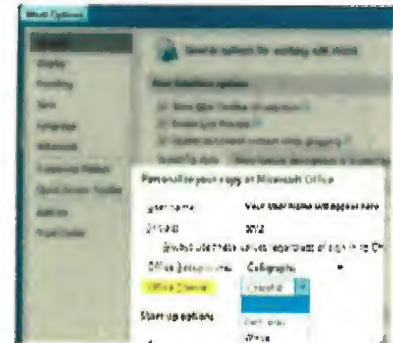
Recheck Box: **Grammar & Style**



How do I change the background color?

There are three **Office Theme** options that will allow you to change the color of the Office 2016 application backgrounds and Ribbons.

1. Click on the **File** tab.
2. Select **Options**.
3. On the Options screen that appears, in the "Personalize your copy of Microsoft Office" section, select the **Office Theme** of your choice.



Outlook

How do I get my "Search" feature to work?

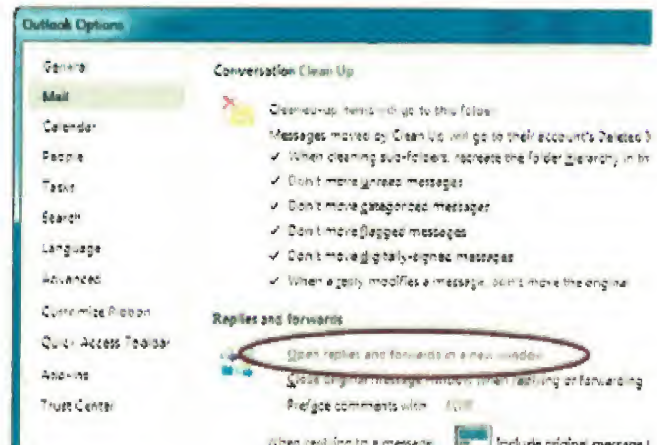
Please contact the EOIR Service Desk and request assistance with your Outlook Search feature.

How do I set Outlook to "Pop-Out" an eMail reply by default?

When viewing eMail messages in the Preview Pane, you are able to Reply or Forward the message from within the Preview Pane.

If you would like for all Replies and/or Forwards to open in a new Window:

1. Select the **File** tab.
2. Select **Options**.
3. Select **Mail**.
4. Scroll down to the **Replies and forwards** section.
5. Check the box next to "Open replies and forwards in a new window"





How do I see messages Older than 12 months?

Outlook 2016's default setting is set to only bring in the last 12 months of eMails.

To view eMails older than 12 months:

1. Under the message that says "**There are more items in this folder on the server**"
2. Click on the link titled "**Click here to view more on Microsoft Exchange**"

Please note: It may take a few minutes to load the older emails.

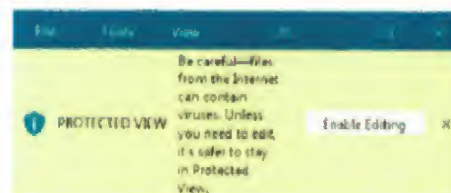


Microsoft Word

Why is my document in Protected View and how do I turn it off?

Documents open in **Protected** view as a security measure put in place by the Department of Justice (DOJ).

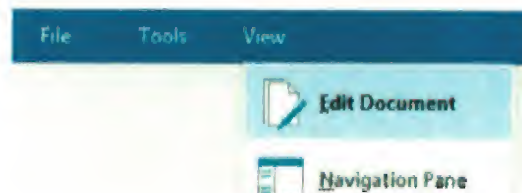
Click on **Enable Editing** on the **PROTECTED VIEW** warning ribbon.



How do I edit Read Only Documents?

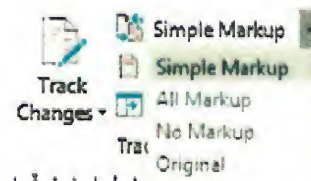
Documents that open in **Read Only** view will only have the **File**, **Tools**, and **View** tabs available.

To edit the document, select the **View** tab, then select **Edit Document**.



How do I view Track Changes?

Select the **Review** tab. In the **Tracking** section, select the desired Markup setting.





Executive Office for Immigration Review Board of Immigration Appeals

Frequently Asked Questions (FAQs) Office 2016 – April 2017

How do I save a document or folder as a Favorite?

To save a **document** as a favorite:

1. Open a new Word document.
2. In the **Recent** items section, hover over the desired document.
3. A push pin will appear next to the document. Click the **push pin**.



To save a **folder** as a favorite:

1. Select **Save As** to save a document.
2. The recently used folders will appear. Hover over the desired folder.
3. A push pin will appear next to the folder. Click the **push pin**.

Lync is now Skype

Lync is now **Skype** for Business.

(b) (7)(E)



Once you have logged in, your information will be retained. **Skype** will automatically launch in the future.





**Executive Office for Immigration Review
Board of Immigration Appeals**

New Features in Office 2016 – April 2017

The upgrade to Microsoft Office 2016 new features for the suite of Office 2016 applications. If there are any questions and/or comments regarding using Microsoft Office 2016 please contact the [BIA ITO Staff](#).

Contents

| | |
|--|----------|
| New Features within Microsoft Office 2016 Overall | 2 |
| New Icons | 2 |
| Welcome Tours..... | 2 |
| Ribbon Icons..... | 2 |
| Outlook..... | 3 |
| New Features when sending an eMail..... | 3 |
| <i>Adding a Screen Shot to an eMail.....</i> | <i>3</i> |
| Available Windows | 3 |
| Screen Clipping | 3 |
| <i>Adding an Attachment to an eMail</i> | <i>4</i> |
| New Features when viewing the Outlook Calendar..... | 4 |
| <i>Calendar at a Glance</i> | <i>4</i> |
| <i>Weather Predictions</i> | <i>4</i> |
| Microsoft Word | 5 |
| Save to Recent Folders..... | 5 |
| Skype..... | 5 |
| Video Call Capable | 5 |



New Features within Microsoft Office 2016 Overall

New Icons

Microsoft Office has rebranded their logo & their color scheme.

The most noticeable change is the **Outlook** icon is now **Blue** instead of Yellow.



Welcome Tours

Three applications in the Microsoft Office 2016 suite, have a "Take a tour" template.

If the template does not appear when opening the application, use the **Search** bar to search for "Welcome". The "Take a tour" option should appear as a search result.



Ribbon Icons

Microsoft Office 2016 has a default view to only **Show Tabs** on the Ribbon. The **Ribbon Tabs and Commands** are hidden by default.

To view the commands for the various tabs:

1. Select the **Ribbon Display Options** button



2. Select **Show Tabs and Commands**






Outlook

New Features when sending an eMail

Adding a Screen Shot to an eMail

Outlook offers a couple of ways to add a screen shot to an eMail message. To attempt either of these, make sure your cursor is in the body of the eMail.

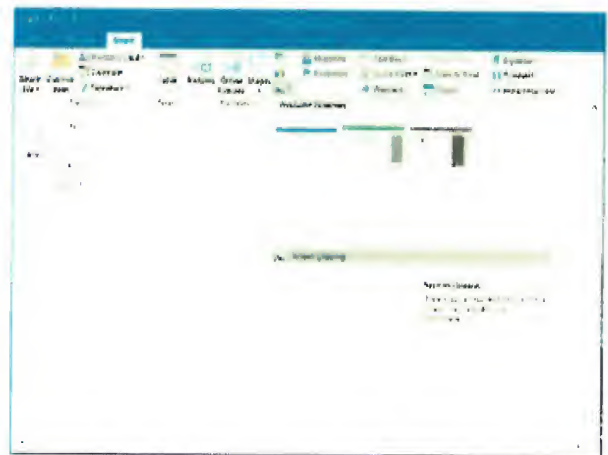
On the **Insert** tab, in the **Illustrations** section, click the **Take a Screenshot** button .

Available Windows


The **Available Windows** section will show:


1. First: Open application windows.
2. Second: Minimized applications windows.
Please Note: these may take a second to load.

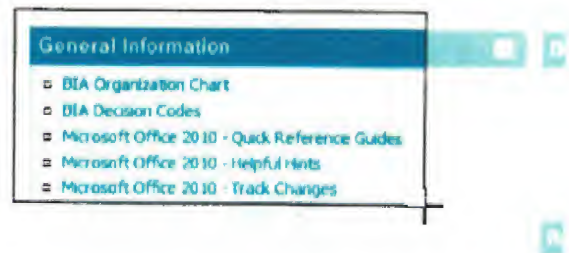
Selecting one of these will insert a screen shot of that window into your eMail.



Screen Clipping

The **Screen Clipping** button  will allow you to take a screen shot of any open screen.

1. Click the **Screen Clipping** button.
2. The screen will become gray, and a plus sign will appear. 
3. Position the **plus sign** in the corner of the image you'd like to capture.
4. Click and hold down the **left mouse button** as you drag the mouse across the area you'd like to capture.
5. Once you unclick the button, the area you selected will appear in our eMail.





Adding an Attachment to an eMail

Outlook has made it easier to find a recent document and attach it to your eMail.

1. On the **Message** tab, click the **Attach File** button.
2. Any document you have recently **Saved** will appear in the list of available attachments.
3. If the document you desire does not appear, use the **Browse This PC...** option.



New Features when viewing the Outlook Calendar

Calendar at a Glance

Outlook retained the icons in the bottom left corner which allow you to navigate between your Inbox, Calendar, Tasks, etc.

When you hover over the Calendar icon in Outlook two things will appear:

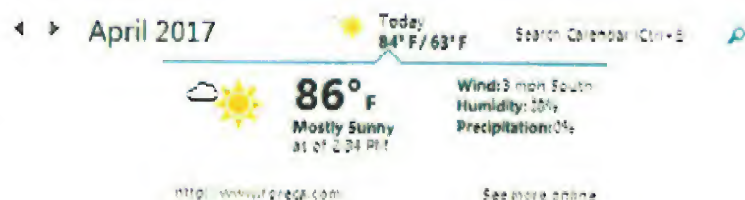
1. A **mini calendar**, allowing you to see the month at a glance;
2. **Upcoming events and meetings** listed on your Outlook calendar.



Weather Predictions

The Outlook calendar now shows the weather at the top of the screen.

Clicking on the **weather** will allow you to see more information, or navigate to more weather information online.





Microsoft Word

Save to Recent Folders

When saving a document, Word displays the recently used folders.

1. Click the **File** tab.
2. Select **Save As**.
3. The recently used folders will appear, grouped by: **Current Folder**, **Today**, **Yesterday**, **Last Week**, and **Older**.



Skype

Video Call Capable

Skype now shows users who are available for video calls.

The overall functionality of Lync has been retained in **Skype for Business**.





**Executive Office for Immigration Review
Board of Immigration Appeals**

Items to Note in Office 2016 – April 2017

The upgrade to Microsoft Office 2016 has resulted in a few look and feel changes that are outlined below. If there are any questions and/or comments regarding using Microsoft Office 2016 please contact the [BIA ITO Staff](#).

Contents

| | |
|--|----------|
| Changes to Microsoft Office 2016 Overall..... | 2 |
| New Icons..... | 2 |
| Welcome Tours..... | 2 |
| File Tab Looks Different | 2 |
| Ribbons Look Slightly Different..... | 3 |
| How do I change the color? | 4 |
| Outlook..... | 4 |
| How do I see messages Older than 12 months?..... | 4 |
| Spelling & Grammar is different..... | 5 |
| Set Outlook to “Pop-Out” an eMail Reply | 5 |
| Microsoft Word | 5 |
| Protected View | 5 |
| Read Only Documents | 6 |
| New Word Document | 6 |
| Track Changes | 6 |
| Warning Message in Word | 7 |
| Save a Document or Folder as a Favorite..... | 7 |
| Lync Changed to Skype..... | 8 |
| OneNote | 8 |



Changes to Microsoft Office 2016 Overall

New Icons

Microsoft Office has rebranded their logo & their color scheme. The most noticeable change is the **Outlook** icon is now **Blue** instead of Yellow.



Welcome Tours


Three applications in the Microsoft Office 2016 Suite, have a "Take a tour" template.

If the template does not appear when opening the application, use the **Search** bar to search for "Welcome". The "Take a tour" option should appear as a search result.

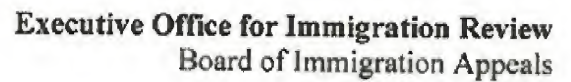


File Tab Looks Different

The **File** tab for the Office 2016 applications appears differently than before.

Instead of showing **File** at the top, there is a **Back Arrow**  which will allow you to navigate back to the previous Ribbon Tabs.





Ribbons Look Slightly Different

Any customizations you have made to your **Ribbon** or **Quick Access Toolbar** should remain.

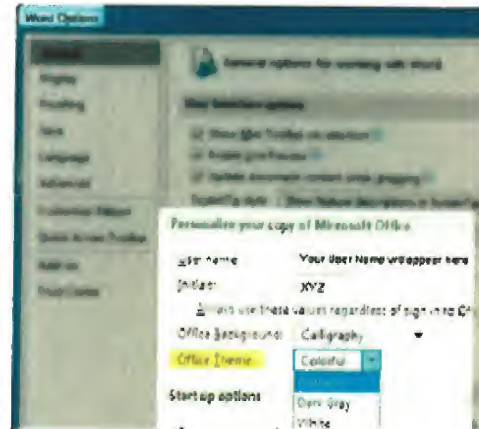
[illegible]



How do I change the color?

There are three **Office Theme** options that will allow you to change the color of the Office 2016 application backgrounds and Ribbons.

1. Click on the **File** tab.
2. Select **Options**.
3. On the Options screen that appears, in the "Personalize your copy of Microsoft Office" section, select the **Office Theme** of your choice.



Outlook

How do I see messages Older than 12 months?

Outlook 2016's default setting is set to only bring in the last 12 months of eMails.

To view eMails older than 12 months:

1. Under the message that says "There are more items in this folder on the server"
2. Click on the link titled "Click here to view more on Microsoft Exchange"

Please note: It may take a few minutes to load the older emails.

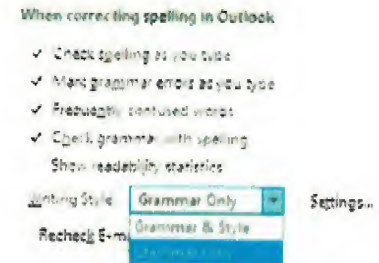




Spelling & Grammar is different

Check your Spelling & Grammar check settings.

1. Under the **File** tab, select **Options**.
2. Select **Proofing**.
3. Under the "When correcting spelling and grammar in Word" section, ensure your settings are set to **Grammar Only**.

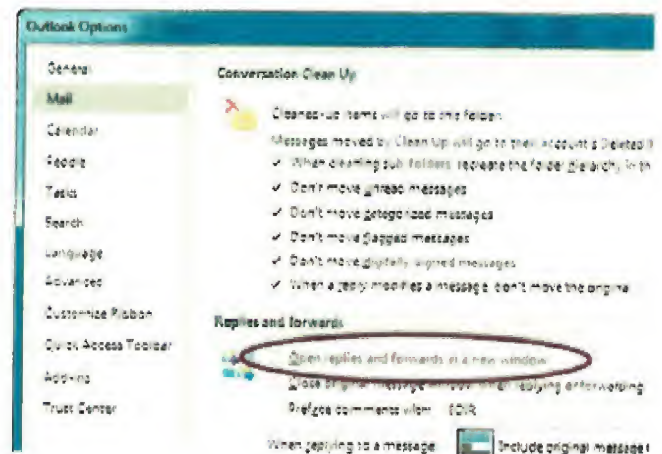


Set Outlook to "Pop-Out" an eMail Reply

When viewing eMail messages in the Preview Pane, you are able to Reply or Forward the message from within the Preview Pane.

If you would like for all Replies and/or Forwards to open in a new Window:

1. Select the **File** tab.
2. Select **Options**.
3. Select **Mail**.
4. Scroll down to the **Replies and forwards** section.
5. Check the box next to "Open replies and forwards in a new window"

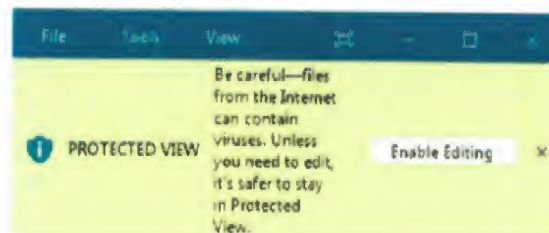


Microsoft Word

Protected View

Some documents may open in **Protected** view.

Click on **Enable Editing** on the **PROTECTED VIEW** warning ribbon.



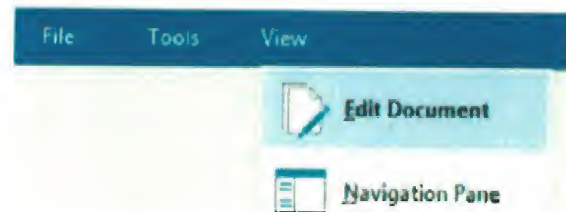


Read Only Documents

Documents that open in **Read Only** view will only have the **File**, **Tools**, and **View** tabs available.

To edit the document:

1. Select the **View** tab.
2. Select **Edit Document**.



New Word Document

When opening a new document in Word 2016, the initial **New Document** screen will appear differently.

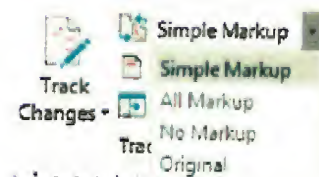
- **Recent Items** will now appear on the left.
- **New Document Templates** will appear on the Right. The first time you open a new document, various document templates will appear. After the first time, you will need to use the **Search** feature to navigate to desired document templates (i.e. Letter template).



Track Changes

The selection for how to view **Track Changes** have changed.

To view **Track Changes**, select **Simple Markup**.





Warning Message in Word

When saving documents originally drafted in an older version of Word (i.e. Word 2010) the Microsoft Word Conversion request notification box will appear.

1. Click the box next to "**Do not ask me again**"
2. Select **OK**.

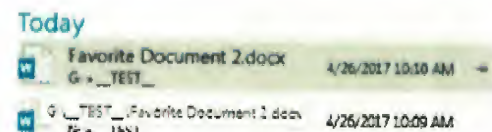
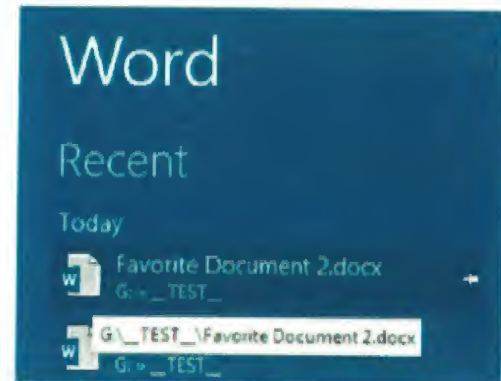


Save a Document or Folder as a Favorite

Office 2016 applications allow you to save a document or a folder as a favorite.

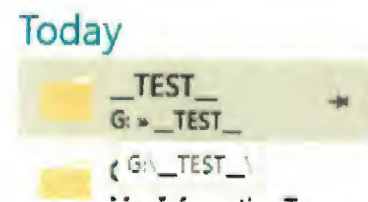
To save a **document** as a favorite:

1. Open a new Word document.
2. In the **Recent** items section, hover over the desired document.
3. A push pin will appear next to the document. Click the **push pin**.



To save a **folder** as a favorite:

1. Select **Save As** to save a document.
2. The recently used folders will appear. Hover over the desired folder.
3. A push pin will appear next to the folder. Click the **push pin**.





Lync Changed to Skype

Lync is now **Skype for Business**.

(b) (7)(E)

Once you have logged in, your information will be retained. **Skype** will automatically launch in the future.



OneNote

When opening links to documents from within **OneNote**, a Microsoft Security Notice appears.

It is ok to click **Yes** for this notification.

